an associated account selected by the electronic device, or otherwise validate access through fast passage gate **650**.

In some embodiments, measures may be taken to ensure that an electronic device does not falsify location information such that location server **620** cannot accurately determine the location of the electronic device. In the fast passage transportation terminal application, a user of the electronic device may attempt to alter the content of the RESPONSE message (e.g., RESPONSE message **232**) with a UWB radio, thus allowing the user of the electronic device to enter into the transit platform area of environment **600** without payment or permission.

To prevent such deceptive and/or fraudulent activity, secure ranging may be used to prevent manipulation of the RESPONSE message, according to some embodiments. A secure transaction subsystem within the electronic device (e.g., secure transaction subsystem **370** of FIG. **3**) may include a hard-coded secure key used to encrypt messages sent to a UWB radio. In some embodiments, the hard-coded secure key cannot be imitated, altered, or mimicked by, for example, the electronic device. The UWB radio may be made aware of the secure key (or a list of possible secure keys) via a database accessible by location server **620** or the UWB radio. The UWB radio may decrypt a message received from electronic devices within environment **600**. In some embodiments, secure ranging can be combined with video imaging techniques to detect fraudulent activity. For example, a non-paying device's location (as determined by secure ranging) can be mapped to a video image of the non-paying device (and associated user) crossing fast passage gate **650**, thus providing visual identity.

FIG. **7** illustrates an example flowchart **700** of operations for an electronic device to select an appropriate credential in a fast passage gate application, according to some embodiments. The operations depicted in flowchart **700** may be performed by an electronic device such as any/all of electronic devices **101**-**104** of FIG. **1**, electronic device **201** of FIG. **2**, or electronic device **300** of FIG. **3**. It is to be appreciated that not all operations may be needed to perform the disclosure provided herein. In some implementations, additional or alternate operations may be performed. Further, some of the operations may be performed concurrently, or in a different order than shown in FIG. **7**.

At **702**, the electronic device receives a "POLL" message from a UWB radio. The POLL message may be an embodiment of POLL message **230** of FIG. **2**.

At **704**, the electronic device responds to the UWB radio with a "RESPONSE" message, which may be an embodiment of RESPONSE message **232** of FIG. **2**. A "FINAL" message, which may be an embodiment of FINAL message **234** of FIG. **2**, may also be received by the electronic device from the UWB radio.

Using the information gathered from the message exchange in operations **702** and **704**, the UWB radio may determine time of flight (ToF) measurements to be used to determine or estimate the location of the electronic device within an environment (e.g., environment **600** of FIG. **6**), such as by using triangulation or trilateration. In some embodiments, the POLL, RESPONSE, and FINAL messages may be encrypted based at least in part on an encryption key stored in a secure subsystem of the electronic device and known to the UWB radio. The UWB radio may send the ToF measurement to a location server (e.g., location server **120** of FIG. **1**, location server **220** of FIG. **2**, or location server **400** of FIG. **4**) so that the location server may determine the location of the electronic device via, for example, triangulation (or trilateration).

At **706**, the electronic device may receive location data from the location server. The location data may be an embodiment of location data **250** of FIG. **2**. The location data may have any format, including formats described above with respect to FIG. **2**.

At **708**, the electronic device may determine if it is near a fast passage gate, such as fast passage gate **650** of FIG. **6**. In some embodiments, the location data received from the location server (at **706**) may be a coordinate that provides a relative location of the electronic device within the environment. The electronic device's location map module, such as location map module **324** of FIG. **3**, may have one or more locations of the fast passage gate within the environment stored in memory. Based on the stored locations of the fast passage gate, the electronic device may determine if it is within a distance less than a predetermined distance from the fast passage gate. In some embodiments, the location data received from the location server may indicate that the electronic device is within a predetermined distance/range from the fast passage gate. If the electronic device does not determine it is not within the predetermined distance/range of the fast passage gate, the electronic device may continue to listen for POLL messages at **702**.

At **710**, if the electronic device determines it is near the fast passage gate, the electronic device may determine a credential to select for a transaction. The credential (e.g., virtual payment card) data may be stored within a secure transaction subsystem on the electronic device such as, for example, secure transaction subsystem **370** of FIG. **3**. In some embodiments, the location map module within the electronic device (e.g., location map module **324** of FIG. **3**) may have information on the card type or types that are compatible with the fast passage gate and select a credential based at least in part on that information. In some embodiments, the location server may send an indication that the electronic device is near the fast passage gate, in which case the indication can also include the credential type(s) that corresponds to the fast passage gate.

At **712**, the electronic device may activate a wireless radio. In some embodiments, the electronic device may not be able to communicate with the fast passage gate via an NFC radio due to a longer distance between the electronic device and the fast passage gate compared to the distance supported by the NFC radio (e.g., about 4 centimeters). In some embodiments, the electronic device may activate a Bluetooth radio, a WiFi radio, an RFID radio, or other such short- or medium-range radio (e.g., radios **338***a*-*n* of FIG. **3**) to perform the communication for a transaction between the electronic device and the fast passage gate. In some embodiments, the electronic device selects the credential (e.g., virtual payment card) before crossing the fast passage gate. In some other embodiments, the electronic device may wait until crossing the fast passage gate into the transit platform area before selecting the credential (e.g., virtual payment card).

At **714**, upon reaching or crossing the fast passage gate, a transaction between the electronic device—using the selected credential (e.g., virtual payment card)—and the fast passage gate is performed. In some embodiments, crossing a virtual line representative of the fast passage gate initiates the transaction, in which, for example, the credential is debited or payment/access validation is otherwise performed. The electronic device can detect crossing the virtual line by determining that its location has changed from a location associated with a general or waiting area of the environment to a location within the transit platform area of the environment, according to some embodiments. In some